Remarks and Arguments

Applicant respectfully requests reconsideration of the present application.

Rejections Under 35 USC §112

Claims 1, 3, 16, 18, 22, 23, 25, 29, 34 and 35 stand rejected under 35 USC §112, second paragraph, as being indefinite.

Applicant has amended the claims and respectfully submits that the claims are now in compliance with §112, second paragraph. No new matter has been added and Applicant requests that this rejection be withdrawn.

Rejections Under 35 USC §102

Claims 1-10, 15, 17, 27-29 and 32-34 stand rejected under 35 USC §102(e) as being anticipated by Hanna, U.S. Publication No. 2002/0136410. Applicant respectfully traverses this rejection as follows.

The present invention is directed to a system and method for providing secure or private communications through the use of ephemeral decryptability of documents, files, and/or messages. In this regard, ephemeral decryptability indicates that the ability to decrypt and encrypted message exists for a finite of time, after which the ability to decrypt the encrypted material is lost. Advantageously, in one embodiment, the present invention provides for a receiving node to decrypt an ephemerally encrypted message, by interacting with an ephemerizer, in a manner in which an eavesdropper would be unable to intercept the decryption keys in an attempt to gain unauthorized access to an encrypted message.

In order for a reference to anticipate a claim, the reference must disclose each and every limitation as recited in the claim. Applicant respectfully submits that Hannah does not anticipate that which is recited in Applicant's claim 1.

Hannah is directed to a method and apparatus for performing ephemeral communication and assuring that an ephemeral decryption key is not accessible subsequent to an expiration time associated with the respective key (Abstract). Hannah discloses that an ephemerizer 60, Fig. 4, is used to decrypt ephemerally encrypted messages. (Paragraph 34). Hannah also discloses that an ephemeral message format

80, as shown in Fig. 5, includes an ephemerizer identifier 82, an ephemeral encryption key identifier 84, and a message key portion 86 that includes a symmetric key encrypted by both an encryption key of the destination party to which the message will passed, as well as by the ephemeral encryption key indicated by the ephemeral encryption key identifier 84. In addition, the message body portion 88 is encrypted with the symmetric key included in the message key portion 86 (see Paragraph 36).

Thus, Hannah discloses a doubly encrypted portion 86 where the symmetric key is encrypted by an encryption key of the destination party and that encrypted value is further encrypted by the ephemeral encryption key.

In contrast, independent claim 1, as amended, is directed to a method of performing secure ephemeral communication comprising receiving, at a first node, a triply wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, the singly wrapped value then being encrypted with a second encryption key to form a doubly wrapped value and the doubly wrapped value being encrypted with a third encryption key to form the triply wrapped value. The triply wrapped value is decrypted using a third decryption key associated with a third encryption key thereby obtaining the doubly wrapped value and the doubly wrapped value is then securely communicated to a second node from the first node. A second decryption key with a predetermined expiration time is obtained at the second node and it is determined if the second decryption key has expired. If the second decryption key has not expired, then the doubly wrapped value is decrypted using the second decryption key to produce the singly wrapped value. The singly wrapped value is then securely communicated from the second to the first node. The first and third encryption keys are the same and the first and third decryption keys are the same and further the first and third encryption keys are associated with the first node.

Applicant respectfully submits that Hannah does not anticipate that which is recited in claim 1 for at least the reason that Hannah does not disclose a triply wrapped value where the triply wrapped value is encrypted with a first encryption key and a third encryption key where the first and third encryption keys are the same and are associated with a node at which the triply wrapped value is received. As shown in Hannah, the message format 80 referenced in Fig. 5 is, at most, a doubly wrapped value.

The Examiner maintains that Hannah teaches multiple ephemerizers that may be used to successfully encrypt the message symmetric key and that this successive encryption reads on the Applicant's decryption of the triply wrapped value. Applicant respectfully disagrees that the successive ephemeral encryption of Hannah to which the Examiner points as anticipating the triply wrapped value of Applicant's claim 1. Specifically, at most the Examiner's position with respect to Hannah would have a triply wrapped value with the value being encrypted with the first encryption key, the singly wrapped value being encrypted with a second encryption key and then the doubly wrapped value being encrypted with a third encryption key, however, the first and third encryption keys, as per the Examiner's interpretation of Hannah, would not be same nor would they be associated with the receiving node.

For at least the foregoing reasons, Applicant respectfully submits that independent claim 1 and its dependent claims 4-7, 9, 10, 15 and 17 are not anticipated by the Hannah references.

Applicant respectfully submits that claims 27, 28 and 32-34 are also patentable over the Hannah reference for at least the same reasons as submitted above with respect to independent claim 1.

Rejections Under 35 USC §103

Claims 11-14 stand rejected under 35 USC §103(a) as being unpatentable over Hannah in view of Official Notice.

Applicant respectfully submits that, for at least the same reasons as submitted above, with respect to independent claim 1, claims 11-14 are not rendered obvious by Hannah in view of Official Notice. Applicant respectfully requests that this rejection be withdrawn.

Claim 16 stands rejected under 35 USC §103(a) as being unpatentable over Hannah.

Applicant respectfully requests that this rejection be withdrawn for at least the same reasons as submitted above with respect to independent claim 1.

Claims 18-21, 23, 26, 30, 31 and 35-26 stand rejected under 35 USC §103(a) as being unpatentable over Hannah in view of Jenkins, U.S. Patent 5,812,669 and in further view of Official Notice.

Independent claim 18, as amended, is directed to a method of performing secure ephemeral communication comprising receiving, at a first node, a doubly wrapped value, the value being encrypted with a first encryption key to form a singly wrapped value and the singly wrapped value being encrypted with a second encryption key to form the doubly wrapped value. An integrity verification key is received at a the first node and is securely associated with the doubly wrapped value. A proof value is communicated from a second node to the first node. A second decryption key that is associated with the second encryption key is obtained and, if it has not expired, the doubly wrapped value is decrypted using the second decryption key to obtain the singly wrapped value. At the first node, it is determined whether or not the second node is authorized to receive the single wrapped value and this determination is a function of the proof value and the integrity verification key. If it is determined that the second node is authorized to receive the singly wrapped value, the singly wrapped value is then securely communicated to the second node.

The Examiner maintains that Hannah teaches a three party system depicted in Hannah, Fig. 9, where one of the nodes serves as an ephemerizer and the other two nodes are involved in message communication. The Examiner asserts that Hannah does not explicitly teach receiving at the first node an integrity verification key securely associated with the doubly wrapped value.

The Examiner maintains that Jenkins teaches a sender computing a digital signature, which then is sent to the recipient that verifies the signature. According to the Examiner, the digital signature of Jenkins reads on proof that a sender is an authorized decryption agent for said value and on verifying the proof by the receiver using the integrity verification key to ascertain whether the sender is an authorized decryption agent for the value.

In order for a claim to be rendered obvious, the cited combination of references must recite each and every limitation of the claim. Applicant respectfully submits that the combination of Hannah in view of Jenkins and in further view of Official Notice does not teach or suggest each and every limitation of Applicant's independent claim 18, as amended.

Jenkins is directed to a method and system for selectively interconnecting a plurality of computers over an open public network and to provide a private secure

computer exchange of EDI interchange communications between a sender computer and a recipient computer. (Abstract). Each of the send computer and recipient computer has an associated public key and an associated private key that are used to provide secure authentication and non-repudiation of both origin and receipt of the secure private EDI interchange communications. (Abstract).

Further, according to Jenkins, the AUTACK or EDI acknowledgement message is used to provide the digital signature in a public/private key system in which the AUTACK is signed by an encrypted hash code from the EDI interchange communication. (Column 1, line 65 – Column 2, line 5). The AUTACK or functional acknowledgement is sealed with the private key of the sender of the functional acknowledgement, i.e. the recipient of the original message. When the original sender decrypts the reply AUTACK message with the recipient's public key, it is assured that the intended recipient actually sent the reply AUTACK or acknowledgement and the integrity of the receipt is confirmed due to the correct hash code being detected. (Column 2, lines 5-14).

Thus, Jenkins is directed to a system for confirming that messages exchanged between a source and a destination are verified as being legitimate due to the use of public and private keys and digital signing thereof.

In contrast, as recited in independent claim 18, at a first node, a doubly wrapped value in addition to an integrity verification key securely associated with the doubly wrapped value are received. A proof value is communicated from a second node, for example, a receiving node, to the first node which then decrypts the doubly wrapped value and determines if the second node is authorized to receive the singly wrapped value.

As an example with reference to claim 18, a message destined from a node A to a node B that requires the ephemeral decryption by an ephemerizer will only be ephemerally decrypted and returned to the node B if node B provides confirmation to the ephemerizer that it is the correct recipient for the information being sent by node A. This determination as to whether or not node B is authorized to receive the message is based on the proof value received from node B as compared to the integrity verification key received from node A. Thus, while node A provides the message and the integrity

verification key in the message sent to node B, it does not receive confirmation back from node B that the message was received.

The cited combination of Hannah in view of Jenkins and Official Notice results in the communication of Hannah with a verified acknowledgement, as per Jenkins, being returned from the recipient node to the transmitting node. The verified acknowledgement is then authenticated based on the public/private key digital signature mechanism. This combination, however, does not result in an ephemeral decryption system where an ephemerally decrypted message is only conveyed to the destination upon confirmation that the destination is authorized to receive it as a function of an integrity verification key transmitted by the sender.

For at least the foregoing reasons, Applicant respectfully submits that the cited combination does not render obvious that which is recited in Applicant's independent claim 18.

Applicant respectfully submits that claims 30, 31, 35 and 36 are not rendered obvious by the cited combination for at least the same reasons as submitted above with respect to claim 18.

Claims 22, 24, and 25 stand rejected under 35 USC §103(a) as being unpatentable over Hannah in view of Jenkins and in further view of Official Notice.

Applicant respectfully submits, for at least the same reasons as submitted above with respect to independent claim 18, that these claims are also not rendered obvious by the cited combination of references.

Applicant believes that the claims are in allowable condition. A Notice of Allowance for this application is earnestly solicited. If the Examiner has any further questions regarding this amendment, the Examiner is invited to call Applicant's attorney at the number listed below. The Examiner is hereby authorized to charge any fees or credit any balances under 37 C.F.R. §1.16 and 1.17 to Deposit Account No. 02-3038.

Respectfully submitted

Paul D. Sorkin Date: 2/28/05

Paul D. Sorkin, Esq. Reg. No. 39,039
KUDIRKA & JOBSE, LLP
Customer Number 045774
Tel: (617) 367-4600 Fax: (617) 367-4656